DETAILED ACTION

Response to Amendment

1. This office action is in response to the RCE/amendment filed 03/31/2008. Claim 6 have been amended; claims 1-5 and 7-38 have been canceled.

Response to Arguments

2. Applicant's arguments filed 03/31/08 have been fully considered but they are not persuasive. Applicant states, see page 3, second to last paragraph, that claim 6 has been amended to include (i) the limitations previously recited in dependent claims 7-10 and 12, and (ii) the new feature "wherein the ASP is operable to pull authentication information from an aggregator using tokens that have been presented by the client to the ASP" (claim6, lines 5-7). Applicant argues, see the last paragraph of page 3, that the combination of prior art references cited by the Examiner do not disclose the combination of features cited in claim 6, and, therefore, the rejection of claim 6 under 35 USC 103(a) has been overcome.

Regarding the limitations recited in dependent claims 7-10 and 12, these claims have been previously rejected, and Applicant has not specifically pointed out how the language of the claims patentably distinguishes them from the references.

Regarding the new feature, although it is not disclosed in the combination of prior art references cited by the Examiner, the feature does not limit the scope of the claim because the language suggests optional but does not require the step to be performed,

i.e., wherein the ASP is **operable to** pull authentication information from an aggregator using tokens that have been presented by the client to the ASP (MPEP 2111.04).

Claim Objections

3. Claim 6 is objected to because of the following informalities:

- "wherein **in** access for the client" (line 4) should be changed to "wherein access for the client".
- "prior to sending **the** response to the client" (the end of the 2nd determining step): there is insufficient antecedent basis for this limitation in the claim. The limitation is interpreted as "prior to sending a response to the client".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mishra et al ("Security Services Markup Language") in view of Gupta et al (6,226,752). Mishra discloses a Single Sign-On (SSO) method wherein an Application Service Provider (ASP) aggregator successfully authenticates a user and then provides a token (i.e.,

name assertion describing the successful authentication) to the authenticated user, who uses the token to access ASPs that have a trusted relationship with the ASP aggregator (page 4, Name Assertion; pages 7-8, Section 3.1, Scenario #1: User-Driven Transactions (Single Sign-On)).

Regarding claim 6, Mishra specifically discloses a method for access management in a distributed data processing system (i.e., controlling access to resources at different business partner sites using Single Sign-On) (pages 7-8, Section 3.1, Scenario #1: User-Driven Transactions (Single Sign-On)), the method comprising:

receiving from a client (i.e., a user's computer) a request to access a net-sourced application hosted by an application service provider (ASP) (i.e., Site B), wherein in access for the client to the net-sourced application is controlled by the ASP on a subscription basis (i.e., user is registered with and authenticated to Site A in order to access a resource protected by Site B) (pages 7-8, steps 3-4);

extracting a logon resource identifier (i.e., verifying the <Issuer> tag comprising a Uniform Resource Locator (URL) identifying the login service of Site A which has a trusted relationship with Site B) from an aggregator token (i.e., the name assertion) that accompanies the request, wherein the aggregator token originated from an ASP aggregator service (i.e., Site A having a trusted relationship with Site B), wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications (i.e., Name Assertion that authenticated user can use to access ASPs), wherein at least one of the net-sourced applications is the net-sourced

application hosted by the ASP (page 8, step 4; page 12, Section 4.1, Name Assertions and Entitlements).

Mishra does not disclose that the ASP is operable to pull authentication information from an aggregator using tokens that have been presented by the client to the ASP; however, this feature does not limit the scope of the claim because the language (i.e., **operable to**) suggests optional but does not require the step to be performed (MPEP 2111.04).

Mishra discloses that the aggregator token is valid only for a period of time (i.e., <ValidityInterval> tag in the Name Assertion) (page 16, see <AuthResponse>). However, Mishra does not teach what the ASP (i.e., Site B) and the ASP aggregator service (i.e., Site A) do if it is determined that the user has not been properly authenticated (i.e., the aggregator token is expired). Specifically Mishra does not disclose: (i) the logon resource identifier is the URL of a login Web page, (ii) determining that the request was not accompanied with a valid application authentication token; (iii) determining that the client or a user of the client has not been properly authenticated; and (iv) sending to the client a response indicating the logon resource identifier as a redirectable destination.

Similar to Mishra, Gupta discloses a method for accessing resource at an ASP (i.e., an application server) protected by a login server, which provides aggregator tokens for accessing the ASP (i.e., the login server authenticates a user and provides the user with a cookie, the user submits the cookie together with a request to access the application server) (fig. 2; Abstract; col. 11, lines 10-38). In addition, Gupta

discloses that if the ASP determines that a user has not been properly authenticated (i.e., the cookie accompanied the request has expired), the ASP will send to the client a response indicating a URL of a login Web page, which is implemented as the default Web page of the login server, as a redirect destination. Gupta also discloses that the login server receives the redirect request, requires the user to successfully complete an authentication process, extracts the identifier of the ASP from the redirect request and sends a response to the client indicating the identifier of the ASP as a redirect destination (fig. 3, steps 302-314; col. 11, line 46 –col. 12, line 49). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Mishra method such that if the ASP determines that a user has not been properly authenticated, the ASP sends to the client a response indicating a URL of a login Web page, which is implemented as the default Web page of the login server, as a redirect destination and the login server receives the redirect request, requires the user to successfully complete an authentication process, extracts the identifier of the ASP from the redirect request and sends a response to the client indicating the identifier of the ASP as a redirect destination, as taught by Gupta. The motivation for doing so would have been that the process does not require any interaction from the user when moving from the ASP to the login server and then back to the ASP (col. 7, lines 19-23). Since the ASP needs the URL of the authentication engine that performs the login service to redirect the user's request and there are more than one authentication engine (figure on page 8), it would be obvious by the combination of Mishra and Gupta above for the ASP

to extract the URL from the token so that the ASP knows which authentication engine the user's request should be redirected to.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gutzmann, "Access Control and Session Management in the HTTP Environment"

Samar, "Single Sign-On Using Cookies for Web Applications"

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Minh Dinh/
Examiner, Art Unit 2132

06/21/08